TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
09/19/2019

SUBJECT:
Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Google Chrome is a web browser used to access the Internet. Successful exploitation of the most severe vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Google Chrome versions prior to 77.0.3865.90

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**
Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**
Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could result in arbitrary code execution. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Details of the vulnerabilities are as follows:

- Use-after-free in UI. (CVE-2019-13685)
- Use-after-free in error. (CVE-2019-13686)
- Use-after-free in media. (CVE-2019-13687)

- Use-after-free in media. (CVE-2019-13688)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser, obtain sensitive information, bypass security restrictions and perform unauthorized actions, or cause denial-of-service conditions.

RECOMMENDATIONS:
The following actions should be taken:
- Apply the stable channel update provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Google:
https://chromereleases.googleblog.com/2019/09/stable-channel-update-for-desktop_18.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13685
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13686
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13687
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13688

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov